

# 為什麼在訪問策略中執行目錄搜尋時找不到受信任域的AD組？

## 目錄

### 問題：

為什麼在訪問策略中執行目錄搜尋時找不到受信任域的AD組？

**環境:**思科網路安全裝置(WSA)、NTLM身份驗證、受信任域

**症狀:**

- 使用者正在嘗試查詢「Active Directory組」，以用作*Policy Member Definition*的一個訪問策略，並且該組未顯示在「Directory Search」（目錄搜尋）中。
- 該組屬於受信任的AD域，而不是WSA已加入的域。

此行為是設計行為。在訪問策略中配置組時，來自受信任域的組不會顯示在*Directory Search*中。

在所有AsyncOS版本中，如果另一個域與WSA加入的域具有雙向信任，則WSA能夠驗證來自其他域的使用者並與各自的AD組匹配。

在這種情況下，可以使用以下步驟在訪問策略中新增受信任域中的組：

1. 瀏覽到GUI —> Web安全管理器 —> Access Policies —> <Policy Name> —> Selected Groups and Users —> Groups
2. 在「目錄搜尋」欄位中手動鍵入整個組名和域名。
3. 按一下「新增」按鈕
4. 按一下「完成」，然後按一下「提交並提交更改」

請注意，如果另一個域與由WSA加入的域沒有雙向信任關係，則WSA將與手動配置的組不匹配

**附註：**在AsyncOS版本7.7及更高版本中，WSA支援多個NTLM領域，對於兩個域之間沒有信任關係的場景，我們可以為第二個域建立一個新的NTLM領域。使用多個NTLM領域，WSA可以從訪問策略中的不同域查詢組。